

JC20 Rec'd PCT/PTO 12 MAY 2005

CLEAN COPY OF SUBSTITUTE SPECIFICATION

CROSS REFERENCE TO RELATED APPLICATIONS

5 This application is a National Stage application under 35 U.S.C. §371 that claims the benefit of PCT/EP2003/012826, filed November 13, 2003, which claims the benefit of Italian Patent Application Serial No. MI2002A002419 filed November 15, 2002. This application claims priority to International Application Serial No. 10 PCT/EP2003012826 and Italian Patent Application Serial No. MI2002A002419.

TECHNICAL FIELD

15 The present invention relates to a method and system for controlling an electronic instrument for metrological measurements.

BACKGROUND OF THE INVENTION

20 As is known, metric instruments are, according to the law, subjected to periodic controls which consist in ascertaining their constant metrological reliability with time, with the aim of protecting the integrity of seals, also electronic, and labels or other protection elements envisaged by the law in force.

25 An authorized person (metric officer) is charged with performing these controls, which refer, for example, to the integrity of both the structure of the measuring instrument, and also to that of the applications or processing programs contained in said instrument.

30 Integrity of the applications means that the applications have not been subjected to interventions which can alter the integrity and originality of the software application which runs the instrument for metrological measurement.

35 Said seals which guarantee the integrity and originality of the application are currently of the hardware type, for example lead seals.

BRIEF SUMMARY OF THE INVENTION

In particular, the present invention relates to a method and system for controlling electronic instruments for metrological measurements including an application for handling the measurement effected by the instrument.

5 Said instrument for metrological measurements can be, for example, an instrument situated inside a gasoline pump, suitable for measuring the flow of gasoline.

For the purposes of the present invention, application for handling the metrological measurement means a
10 software or a processing program which can acquire, process, visualize and print the data relating to the measurement effected.

The Applicant has observed that for these controls the operator (metric officer) must go to the place where
15 the measurement instrument is installed and check the integrity of said hardware seals. Should the supplier of the application issue a new updated version of said application, the metric officer must go on site to remove said seals and insert the new ones, after verifying the
20 correct functioning of the updated version of the application.

The intention of the Applicant is to simplify certification operations of software applications for electronic instruments for simple metrological measurements
25 and make them reliable.

The Applicant has achieved a method and system for controlling an electronic instrument for metrological measurements, wherein a control application, residing on a computer connected to said measurement instrument, for
30 example through a network, checks whether the handling application of the measurement effected by the instrument has undergone alterations, violations, modifications or similar variations. This control of the handling application of the instrument results in the emission of an authenticity stamp.
35

The control application preferably determines whether the handling applications satisfy the following

conditions:

- * the handling application installed on the instrument must conform with what is certified at the start of the instrument;
- 5 * the handling application installed on the instrument cannot be unduly interfered with;
- * any variation in the handling application installed on the instrument must be evident and acknowledgeable;
- * the presence of a different handling application
10 must be acknowledgeable;
- * the techniques adopted must guarantee that all the aforesaid actions are carried out in a context of data security, using suitable cryptography techniques, digital signatures, certifications etc..;
- 15 * all relevant actions in the sphere of variations in the programs which can be effected by the instrument, must be marked on carriers that cannot be modified by third parties.

20 The controls are generally such as to allow a definite reconstruction of the actions effected on the handling application of the instrument.

An aspect of the present invention relates to the controlling system of an electronic instrument for metrological measurements, including a local processing computer which comprises a handling application of said instrument, characterized in that it includes a control application for said handling application, which can be associated with said local computer, said control application being suitable for generating a univocal certification code for the application.
30

A further aspect of the present invention relates to a method for controlling an electronic instrument for metrological measurements, said instrument being associated with a local processing computer including a handling application of said instrument, comprising the following steps:
35

- * receiving, at the start of the handling application,

information contained in said local unit referring to the handling application;

- * processing said information through a comparison with pre-memorized information;

5 * issuing a univocal certification code which can be associated with said handling application;

- * printing on paper a stamp containing said univocal code.

The characteristics and advantages of the method and
10 system for controlling metrological measurement instruments according to the present invention will be better clarified and appear more evident from the following illustrative and non-limiting description of an embodiment, with reference to the attached figures, wherein:

15 **BRIEF DESCRIPTION OF DRAWINGS**

figure 1 is a block scheme of the control system according to the present invention applied to generic client uses;

figure 2 is a block scheme of the control system according to the present invention applied to a fuel station for motor vehicles;

figure 3 is a representation of a "software stamp" according to the present invention;

figures 4a-f represent visualization cards of the control application according to the present invention.

25 **DETAILED DESCRIPTION OF INVENTION**

With reference to the aforesaid figures, the system according to the present invention preferably comprises a central processing unit (server) (2), and at least one
30 local processing unit (3) in which there is at least one handling application of a metric instrument (4). This central processing unit preferably also includes a handling application of a metric instrument (4).

The connection between said central unit and the local units is preferably obtained through a traditional telecommunication network, a LAN network, for example, an Ethernet network, or an Internet connection. In general

said network allows applications and programs, physically residing in a memory of said central processing unit, to be used in said local units.

Figure 1 shows, as an example, three local stations, as the system of the present invention is also capable of controlling a series of local units contemporaneously. One of the local units indicated in figure 1 comprises two handling applications (4) of an electronic instrument for metrological measurements, as the system of the present invention contemporaneously and equivalently controls one or more applications inside the local unit itself.

Said central processing unit preferably includes at least one control application (21) of said handling applications, in addition to at least one central application (22).

At least one dynamic library (6) of functions which can be associated with said control application (21), is preferably present on both the central processing unit and the local units, said library acting as a connection between the handling applications and the control application.

Figure 2 shows an application example of the control system according to the present invention, applied to a fuel station for motor vehicles, indicated, as a whole, with reference number (7).

The fuel station includes at least one gasoline pump (71), containing inside said metrological measurement instrument, suitable for measuring the flow of gasoline from a pump. A local processing unit associated with said pump includes said handling application, as described above, which controls the measurement instrument.

Said fuel station also includes an automatic distribution pump (72), suitable for allowing the pumps to operate in the absence of personnel. This pump is activated by inserting a certain amount of money, in the form of banknotes or credit cards, bancomat or similar. Inside

this column there is, for example, a further local processing unit.

Other local processing units are situated, for example, in sales and/or distribution points of products (74) of the fuel station, accounting and/or administrative offices (75).

According to the example of figure 2, the central processing unit (73) connects the aforementioned local processing units so as to form a network.

10 According to the present invention, the control application is preferably contained in the central unit (73). Alternatively, if the fuel station is not connected by a network, but comprises at least one local processor associated with a metrological measurement instrument, 15 said control application is installed inside said local unit.

The handling application of the measurement instrument preferably comprises an authenticity certification, which is provided by the application author. This certification includes a digital signature which is implemented, for example, by means of an RSA cryptography protocol.

This digital signature, through a mechanism of public and private keys, guarantees the authenticity of the handling application with which said key is associated.

25 A technological note which implements said digital signatures is the Microsoft® Authenticode™ technology which verifies that a certain application has a valid certificate, or that the identity of the application producer corresponds to what is certified and that the certificate is still valid. This is achieved by applying a digital signature to the software code, which allows remote clients to check the reliability of the application editor.

35 According to the present invention, the control application is capable of reading said digital signatures and acknowledging their authenticity. If said authentic-

ity is not verified, the control application emits a signal and interrupts the start of the handling application which contains the non-valid digital signature.

Furthermore, the control application acquires some
5 information on the unit on which the application to be controlled resides, in order to create a single data bank, connected to the unit itself. Possible examples of information which can be useful for controlling the application are:

- 10 • series number of the network card,
- series number of the hard disk,
- univocal identification of the data processor, etc..

In the case of network configurations, the control
15 application also univocally identifies the machines connected by the network through their local application component, so as to be able to react to any possible variations in the network configuration.

Once the aforementioned information has been acquired, the control application processes all the data
20 and creates a synthesis of a limited dimension. This synthesis can be obtained, for example, by means of so-called cryptography "hashing" algorithms (SHA, RSA, etc..) and generates a univocal code which is called "software stamp", which is printed from these local units and associated with the controlled handling application.
25

This univocal code is preferably printed, for example, in the form illustrated in figure 3, which refers to the certification of a handling application called SINP,
30 version 2.0.1, produced by the same Applicant and granted on September 13, 2001. This stamp (8) also shows a stamp printing date (81), a fuel station code (82), a bar code (83) corresponding to said univocal code of the software stamp.

35 The handling application operates as follows.

At the start of the handling application (4) to be

controlled, the control application (21) is automatically called by means of said dynamic library (6) associated with the handling application in the local unit.

Information on the handling application itself is
5 acquired through said library.

The application is validated using the verification of said application certificate, for example according to the rules of the Microsoft® Authenticode™ standard.

The control application (21) acquires some information on the local processing unit (3) on which the handling application (4) resides, in order to create a single data bank for recognizing the unit itself. In the case of network configurations, the handling application also univocally identifies the other units present on the
10 network, through all dynamic libraries (6) present in
15 each local unit, so as to be able to react to any possible variations in the network configuration.

Once all the aforementioned information has been acquired, a "software stamp" is emitted, as described
20 above, which is memorized in said local processing unit and bound to the controlled handling application.

All the applications effected by the control application on the handling application to be controlled, are preferably collected in a file, whose integrity and consistency is checked in order to verify that no cancellations or manipulations have been made. Any possible inconsistencies found in this phase, produce a signal and prevent the start of the applications.
25

If an updating of the handling application is desired, for example by installing a new version, the control application emits a new software stamp.
30

In particular, the control application detects that the application has changed and is no longer consistent with the information pre-installed through the software stamp. In this case, the authenticity of the new version
35 of the handling application is checked.

This control is essentially carried out in three

steps:

- a control is made that the new version has been prepared by the same producer as the previous one, through said digital signature;
- 5 • a control is made that the new version is subsequent to the previous one (for example version 1.2 in the place of version 1.1);
- a control is made that said version is consistent with the other applications, with which it operates,
- 10 of the local processing unit.

Once the above controls have been effected, the control application proposes to the user to produce a new software stamp. The software stamp represents the necessary evidence, on a normative level, for the correct handling of the issuing of new versions. All the above is
15 obtained, in concrete terms, through a printout on paper which produces a model as illustrated in figure 3.

Figures 4a-e represent a few examples of insertion and/or visualization masks generated by the control application during a survey on a handling application.
20

Figure 4a illustrates a first mask (91), which, at the start of the handling application of the measurement instrument, shows the univocal code of the software stamp. In this case, there was no modification in the handling application, and the handling application is
25 consequently correctly started by pushing the key "OK". This mask is optional, in the sense that it can be put in evidence when the handling applications envisage the presence of a user at the start; when the start of the handling application is automatic, for example in correspondence with the tensioning of a plant, this mask is
30 omitted.

Figure 4b illustrates a second mask (92), which shows that there has been a change in the configuration of the local processing unit. This change can, for example,
35 be an update of the handling application version or

a change in the hardware and/or software configuration of the processing unit.

In this case a comparison mask (93) is put in evidence, in which these changes are listed. In particular,
5 an upper box (931) of said mask reveals the new applications and/or versions of the application present on the local unit, and a lower box (932) reveals the substituted parts. The new configuration revealed by said upper box, must be confirmed by a push button present on the lower
10 part of the card; the confirmation operation simply declares that the changes comply with the aforementioned authentication conditions. After this confirmation, a new univocal code is issued and a new software stamp is printed.

15 The univocal code can, at this point, be inserted in said second mask (92) and, following confirmation, by pushing the key "OK", the system proposes a third mask (94) in which a confirmation is required (yes/no) that the modifications comply with the regulations on the metric
20 test of the measurement instrument.

In the case of confirmation (yes), the system proposes a fourth mask (95) which communicates that the operations have been correctly effected and allows the correct start of the handling application.

25 In the case of lack of confirmation (no), the system proposes a fifth mask (96), which communicates the impossibility of correctly starting the application, as the metrological operations have not been completed.

In this case, the application can only be started for
30 effecting functional tests.

The application is preferably developed according to modularity, re-use of the code and portability criteria, in order to guarantee the natural evolution which the control application will undergo during its life cycle.
35 Respect of these requirements guarantees the possibility of adding new functions with limited impacts. For this purpose, when applicable, the use of programming lan-

guages of the type known as "object oriented", is preferable.

It is preferable, moreover, to use techniques which allow the application and the data format to be as independent as possible of each other. In this way, the application is ready for any possible data format changes and is advantageously compatible with other applications, devices or systems.

All public interfaces, public data and functions are documented, in order to guarantee access to the control application code. The system variables preferably have mnemonic names and respect the code writing notations typical of the development environment (prefixes for indicating the data type, etc..). Each public function or method is suitably documented through a description on the function itself, and a functional description is specified for each parameter, including the validity interval and the use in input or output of the parameter itself.

The error codifications are preferably consistent with the remaining parts of the application and can be obtained from a single source (header file or resource). In any case, any error code which can be generated by the application is documented and memorized in the application event register.

Respect of the application longevity requirement inevitably implicates the selection of architectures which are presumably supported for a period of time equal or longer than the assumed life of the application itself.

The control application, according to the present invention, follows the operation modes, terminology and documents already known to users of the handling application and metrological measurement instrument, as much as possible, so that the user itself can consider the procedure as "familiar". In any case, the interfaces and designs of the masks are as simple and clear as possible. The most frequent operations are advantageously effected

with the lowest possible number of passages. All operations of the control application are coherently grouped into functional sets, to make them easily available. Access to the functions is preferably obtained by means of
5 buttons or, when applicable, through menus, hyper-tests or icons.

The parts indicating commands or data must have sufficient dimensions to allow them to be clearly read. The dimensions of the interface elements should not however
10 be too large, in order to prevent the elements themselves from becoming dispersive.